**网络安全威胁事件交互工具**

**会议记录**

1. **时间**

2016.11.24 周四 15:30~16:30

1. **参与人员**

姚原岗老师、张天野、高翔、丁铁成、关会华

1. **会议内容**

本次会议围绕以下若干点内容展开，分别是：

1. **初始状态输入初始节点时，按回车无响应**

建议在添加节点时，增加键盘“回车”键的事件响应；

1. **页面刷新时，系统直接返回页面默认的初始状态，误清空已有操作**

建议在检测到页面刷新行为时，对用户进行提醒，是否要保存当前图等其他信息，防止因为误操作导致的分析内容遗失；

1. **在现有图结构基础上，增加数据库表中不存的节点及边，数据同样能够保存于txt 图文件中**

目前系统仅能够添加库表中存在的节点，建议增加添加虚拟节点或边的功能，实现分析流程的完整（需要对虚拟节点和现实节点进行标记区分，例如在节点信息中添加一个表示虚拟节点或者现实节点的字段）；除此之外，虚拟节点及边的信息仍然能够添加入图的数据结构中，得以保存；

1. **图标、结构、响应交互仿maltego**

建议在界面风格和系统交互上，多多参考maltego；

1. **提高图结构数据的可视性**

建议在节点较多的情况下，将节点抽象为一个点，通过缩放功能，进一步展现节点的icon及key value（例如www.baidu.com）；除此之外，key Value的显示与否可以通过设置按钮进行控制；

1. **节点／边选择及删除的逻辑**

建议仔细考虑节点及边的选择及删除逻辑，例如批量选择及批量删除；

1. **增强属性列的可读性**

建议对节点及边的属性名称进行汉化处理，除此之外，默认值为null的属性可以暂时不予显示；

1. **历史记录返回后，无法撤销**

当前对历史记录回撤之后，无法撤回上一步操作；建议增加回撤操作；

1. **域名URL、邮件地址等解析，如包含多条内容的解析**

能够对数据库表中某项的值进行解析，例如将包含了多条url的项进行处理，提取出其中每一条数据；

1. **展示效果，不要“动态漂移”，节点、边的互不遮挡**

建议停止力引导图的抖动，思考如何解决节点和边过多时带来的遮挡问题；

1. **图结构无法平移**

建议增加平移交互；

1. **如何保留、展示关键路径**

与6）相关，可以批量删除无关节点，或者是隐藏无关节点；

1. **统计视框的逻辑及效果可用性**

暂时保留统计视图部分，不进行讨论；

1. **如何从视图中查找已有节点**

建议增加查找点的功能；

1. **节点间边关联查询不反馈**

查询结果不存在是添加反馈；建议增加另外一个新功能，用来查询图结构中两个无关节点是否在数据库表中有关联；

1. **查询结果反馈数量的提示／无返回的提示／其中部分已存在于图中的提示**

建议对查询结果的数量进行提醒；

1. **数据导入与已有数据冲突、合并、替换、融合的处理策略**

考虑在数据导入过程中出现的各种问题及处理策略，如题；

1. **数据库表的可见性。**

建议在初始状态下，能够让分析人员看到数据，选择数据，而不只是输入待查数据。如按照时间看到各表／实体的数据队列，一边选择较近导入的新数据。

1. **选择并保存部分图结果；选择并仅显示选择的局部图并基于此进行进一步的交互分析（就是选择删除？）。**

与6）、12）相关；

1. **主题themes**
2. **数据导入不全**

经过沟通发现是导入的数据表不同；

1. **地图再说**

后期会将有关地理位置的库加入，目前暂不讨论；

1. **树状结构时，会出现断层**

由于处理逻辑不同而导致的结果，可更改；

1. **任务讨论**

由于增加了一些新的功能，我们需要对目前系统的功能进行提炼，并对系统的布局进行调整。

系统中将添加菜单栏，菜单栏包含以下内容：

|  |  |  |
| --- | --- | --- |
| **一级菜单** | **二级菜单** | **三级菜单** |
| 文件 | 保存 |  |
| 打开 |  |
| 库表查看 |  |
| 搜索 | 搜索关联的全部 |  |
| 搜索关联的邮箱 |  |
| 搜索关联的域名 |  |
| 搜索关联的ip |  |
| 搜索关联的样本 |  |
| 查询 | 查询点 |  |
| 查询两点之间路径 |  |
| 查询两点之间关联 |  |
| 选择 | 选择边 |  |
| 选择点 | 选择所有邮箱 |
| 选择所有域名 |
| 选择所有ip |
| 选择所有样本 |
| 编辑 | 添加节点 |  |
| 删除节点 |  |

此外，系统中所支持的交互及操作有，需要对这些功能进行完善和修改：

|  |  |
| --- | --- |
| 图交互 | 平移 |
| 缩放 |
| 节点交互 | 单选 |
| 刷选 |
| 拖拽 |
| 右键 |
| 图操作 | 结构切换 |
| 节点操作 | 新增 |
| 删除 |
| 寻找链接 |

本周将完成讨论内容的2）、5）、6）、7）、8）、16），并着手对设计新的界面。